Informationssicherheits-Richtlinie für Lieferanten

	Freigabe Vorwerk Gruppe	Freigabe Vorwerk Gruppe	Freigabe Vorwerk Gruppe
Bereich	Global Director Purchasing	Global Director Quality	Informationssicherheits-Beauftragter
Name	Hr. Czayka	Hr. Schröder (QMB)	Hr. Münstermann (ISB)
Datum	01.11.2022	01.11.2022	01.11.2022
Unterschrift			

Inhalt

1. Einleitung

Die Vorwerk-Autotec & Drivetec-Gruppe - im Folgenden Auftraggeber genannt, beliefert viele Automobilkunden mit Produkten unterschiedlicher Anforderungen und Funktionen.
Zur Erfüllung der aktuellen und künftigen Anforderungen unserer Kunden und Gesetzgeber sowie der Absicherung des Unternehmens gegen Cyberkriminalität sind Aspekte der Informationssicherheit immer stärker zu berücksichtigen.
Diese Informationssicherheitsrichtlinie (ISR) bildet den verbindlichen Rahmen zwischen Auftraggeber und Lieferant, und dient dazu, den Anforderungen an den Schutz von Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit gerecht zu werden.
Dieses Dokument ist Bestandteil unserer Einkaufsbedingungen und die Bestätigung durch den Lieferanten die Voraussetzung für die Belieferung an unseren Unternehmensverbund.

Im Widerspruchsfall gilt die deutsche Fassung.

2. Anwendungsbereich

Die vorliegende ISR gilt für alle Lieferanten und Dienstleister unseres Unternehmesverbundes:

Vorwerk Autotec GmbH & Co. KG - Wuppertal
Vorwerk Drivetec GmbH - Wuppertal
Vorwerk Autotec Polska Sp. z o.o. - Brodnica
Vorwerk Autotec (Suzhou) Limited
Vorwerk Drivetec (Suzhou) Limited
Vorwerk Autotec de México S.A. de C.V. – Lagos de Moreno
Vorwerk Autotec Serbia d.o.o. - Cacak
Vorwerk Drivetec Serbia d.o.o. – Cacak

3. Informationssicherheit in Lieferantenbeziehungen

Vorwerk arbeitet ausschließlich mit Auftragnehmern zusammen, welche sich eigenständig zur grundlegenden Wahrung der Vertraulichkeit von Informationen und Geschäftsgeheimnissen verpflichten. In Einzelfällen, wenn die übergebenen oder geteilten Informationen einem gesteigerten Sicherheitsbedürfnis unterliegen, können darüber hinaus besondere Maßnahmen von Auftragnehmern gefordert werden, um dem gesteigerten Sicherheitsbedürfnis Rechnung zu tragen. Dies wird zumeist im Rahmen von Geheimhaltungsvereinbarungen geschehen.

4. Allgemeine Anforderungen

4.1. Grundsätzliches

Der Auftragnehmer wird aufgefordert sein Managementsystem, um die Grundsätze der Informationssicherheit zu erweitern. Dabei können Standards wie ISO/IEC 27001, VDA ISA Katalog oder BSI IT-Grundschutz als Grundlage dienen. In Einzelfällen kann eine externe Zertifizierung, ein bestandenes TISAX-Assessment oder Eigenbeurteilung zur Voraussetzung für bestimmte Geschäftsbeziehungen werden.

4.2. Interne Organisation

Es sind Richtlinien, Prozesse und Verantwortlichkeiten zu definieren, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.
Dies beinhaltet insbesondere:

- Die Erstellung einer Informationssicherheitsrichtlinie.
- Anwenderrichtlinien zur Festlegung von Regeln für den Umgang mit Anwendungen, Systemen und IT-Endgeräten und dem Verhalten bei der Nutzung von Informationstechnologie
- Die Beschreibung von Prozessen für die Verwaltung von Datenträgern, Dokumenten und Informationen.
- Die Festlegung der Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit.

- Die Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses.
- Die regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen

4.3. Physische und umgebungsbezogene Sicherheit

Der Auftragnehmer hat dafür Sorge zu tragen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationen von Vorwerk verarbeitet werden, ausgeschlossen ist. Dies gilt weiterhin auch für Anlieferungs- und Ladebereiche, über die unbefugte Personen die Räumlichkeiten betreten könnten.
Von Seiten des Auftragnehmers sind Richtlinien zu erstellen, die aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung regeln.

4.4. Schutz von Informationswerten

Der Auftragnehmer ist aufgefordert seine Informationswerte zu erfassen, auf ihren Schutzbedarf zu bewerten und erforderliche Maßnahmen je nach Risikoklasse umzusetzen.
Vorwerk verwendet eine Kennzeichnung seiner Informationswerte. Mit „vertraulich“ oder „streng vertraulich“ gekennzeichnete Dokumente, als auch solche deren Inhalt in der üblichen Geschäftswelt von sensiblem Wert sind, dürfen nur ausgewählten Mitarbeitern zugänglich gemacht werden. Mit „intern“ gekennzeichnete Dokumente sind für die Geschäftsbeziehung zwischen Auftragnehmer und Auftraggeber bestimmt und im Unternehmen frei verteilbar.
Im Grundsatz gilt:

- Sowohl Daten als auch die Träger dieser Daten sind vor Verlust, Zerstörung, Manipulation und unberechtigten Zugriff zu schützen. Nicht mehr benötigte Datenträger sind nach sicheren Verfahren zu vernichten.
- Der Datenaustausch darf nur über von Vorwerk freigegebenen Datenaustauschwegen durchgeführt werden.
- Es ist durch die Partnerfirmen sicherzustellen, dass keine unberechtigten Dritten vertrauliche Informationen mithören können oder Einsicht in diese erhalten. Beabsichtigt der Lieferant eine bewusste Weiterleitung ausgewählter Information an Dritte, so ist eine Freigabe von Vorwerk einzuholen. Dies gilt insbesondere für Informationen zu Projekten, die mit einer Geheimhaltungsvereinbarung verbunden sind. Beim Versand von E-Mails ist der Verteilerkreis auf das nötige Maß einzuschränken.

4.5. Sicherheitsrelevante Vorfälle

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) mit potenziell negativem Effekt zu implementieren.
Dies beinhaltet insbesondere:

- Die unverzügliche Meldung von Informationssicherheitsvorfällen an den Auftraggeber, insbesondere bei Bekanntwerden sogenannter Cyberangriffe.
- Die Protokollierung von Sicherheitsvorfällen.
- Die Implementierung von Prozessen zur Einleitung von Maßnahmen zur Verhinderung / Wiederholung von Informationssicherheitsvorfällen

4.6. Schwachstellen- und Patchmanagement

Eine Ausnutzung technischer Schwachstellen sind durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines geregelten Patchmanagements zu verhindern.
Es sind regelmäßige Überprüfungen zur Erkennung von Schwachstellen der IT-Struktur bei Bedarf auch durch externe IT-Berater durchzuführen.

4.7. Datensicherungen

Es sind Maßnahmen umzusetzen, die gewährleisten, dass schutzbedürftige Informationen und Daten / personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

4.8. Kryptographie

Der Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

4.9. Arbeiten außerhalb der Organisation

Der Auftragnehmer hat für seine Beschäftigten eine Richtlinie zu erstellen, welche das Arbeiten außerhalb der Organisation regelt. Der Fokus muss auf der Vertraulichkeit der Daten liegen und verhindern, dass Unbefugte Informationen abhören, erblicken, physisch stehlen oder elektronisch abgreifen können.

4.10. Notfallmanagement

Die Systemverfügbarkeit muss in schwierigen Situationen, wie Krisen- oder Schadensfällen, aufrechterhalten bzw. schnellstmöglich wieder hergestellt werden. Der Lieferant muss für die kritischen Informationswerte und IT-Systeme Notfallpläne erstellen, um die weitere Geschäftstätigkeit zu gewährleisten. Diese Notfallpläne müssen regelmäßig auf ihre Wirksamkeit getestet und ggf. optimiert werden.

5. Besonderheiten für Organisationen mit Zugang zum Netzwerk

5.1. Umgang mit Anmeldeinformationen und -medien

Anmeldedaten dürfen an unautorisierte Personen nicht weitergegeben werden. Bereits beim Verdacht der Kompromittierung sind die Zugangsdaten zu ändern und der Vorfall zu melden. Solange ein Zugriff auf das Vorwerk Netzwerk besteht, ist ein Verlassen des Arbeitsplatzes verboten.

5.2. Zugriffsrechte

Zugriffsrechte auf Systeme von Vorwerk müssen beantragt werden. Zugriff auf Daten von Vorwerk dürfen den Mitarbeitern nur nach dem Need-to-Know-Prinzip zugänglich gemacht werden.

5.3. Umgang mit Informationen

Alle Informationen sind unter der grundsätzlichen Annahme, dass diese streng vertraulich sind zu behandeln. Eine lokale Speicherung von Informationen und Daten ist verboten. Anpassungen und Updates an Software und IT-Systemen müssen bei den Ansprechpartnern von Vorwerk angemeldet und freigegeben werden.

6. Besonderheiten für Softwarelieferanten

Die gelieferte Software darf keine Funktionen erhalten, die die Schutzziele der Daten als auch der Software selbst gefährden insbesondere dem unerwünschten Ein- und auch Ausleiten von Daten und Funktionen oder der unerwünschten Veränderung von Daten bzw. der Ablauflogik. Der Lieferant hat nach Stand der Technik zu überprüfen, dass keine möglicherweise schadenstiftende Software (z.B. Viren, Würmer, Trojaner) mitgeliefert wird.

7. Liste der Änderungen

Datum	Index	Beschreibung der Änderung
2022-11-01	A	Erstausgabe